UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case Number 25-20165
Honorable David M. Lawson

MATTHEW WEISS,

Defendant.
_____/

OPINION AND ORDER DENYING DEFENDANT'S "OMNIBUS" MOTION TO DISMISS INDICTMENT

Defendant Matthew Weiss is charged in a 24-count indictment with unauthorized computer access and aggravated identity theft stemming from allegations that he hacked into the internet accounts of student athletes at the University of Michigan, where he coached football, and elsewhere, downloading personal identifying information and photographs. He has moved to dismiss several counts of the indictment, arguing that some counts are duplicitous (charging more than one offense in a single count), others are multiplicitous (charging the same crime in several different counts), and still others do not allege venue sufficiently. Because none of these arguments merit dismissal of the charges, the motion will be denied.

I.

The indictment alleges that from approximately 2015 through January 2023, Weiss unlawfully accessed the "social media, email, and/or cloud storage accounts" of more than 3,300 individuals, most of whom were female college athletes, by guessing or resetting their passwords. Indictment, ECF No. 1, ¶¶1-2. As part of this scheme, Weiss allegedly gained unauthorized access "to student athlete databases of more than 100 colleges and universities across the country that were maintained by Keffer Development Services, a third-party vendor." *Id.* at ¶6. He did this by "compromising the passwords of accounts with elevated levels of access, such as the accounts of

trainers and athletic directors." *Ibid.* Weiss downloaded personally identifying information and medical data of more than 150,000 athletes from the Keffer databases. *Id.* at ¶7. He also downloaded the encrypted passwords of certain athletes and decrypted them using techniques he learned on the internet. *Id.* at ¶8. He combined what he obtained from Keffer with personal information found elsewhere online — such as athletes' "mothers' maiden names, pets, places of birth, and nicknames" — to guess or reset the passwords of over 2,000 athletes. *Id.* at ¶¶9-10. He also accessed the social media, email, and cloud storage accounts of over "1,300 additional students and/or alumni" from colleges nationwide, in some instances by exploiting weaknesses in authentication processes. *Id.* at ¶¶12, 14. He allegedly used his access to the accounts to download users' "personal, intimate digital photographs and videos" without their knowledge. *Id.* at ¶3.

The grand jury returned its indictment in March 2025. Counts 1 through 10 allege that Weiss obtained access to the social media, email, and cloud storage accounts of 10 Jane Does "without and in excess of authorization," in violation of 18 U.S.C. §1030(a)(2)(C) and (c)(2)(B)(ii), by accessing servers operated by the University of Michigan or one of several unnamed technology providers. A table in the indictment summarizes the dates, targeted individuals, and targeted servers alleged in each of the first ten counts:

Count	Date (in and around)	Targeted Individual	Targeted Server
1	May 2021 to January 2023	Jane Doe #1	Unknown Technology Provider
2	July 2021 to January 2023	Jane Doe #2	Technology Provider #1
3	October 2022	Jane Doe #3	Technology Provider #2
4	December 2022	Jane Doe #4	University of Michigan
5	December 2022	Jane Doe #5	Technology Provider #3
6	July 2022 to January 2023	Jane Doe #6	Unknown Technology Provider
7	October 2022	Jane Doe #7	Technology Provider #1
8	September 2021	Jane Doe #8	Technology Provider #1
9	August 2021 to January 2023	Jane Doe #9	Technology Provider #1
10	November 2022	Jane Doe #10	Technology Provider #1

ECF No. 1, PageID.5. Counts 11 through 20, which the defendant challenges only on venue grounds, allege aggravated identity theft under 18 U.S.C. § 1028A(a)(1), based upon the same unauthorized logins described in Counts 1 through 10.

Count 21 alleges an additional violation of 18 U.S.C. §1030(a)(2)(C) and (c)(2)(B)(ii) based upon Weiss's alleged intrusion into "approximately 150 accounts" on virtual server space rented by Keffer Development Services. Count 22 alleges unauthorized access to the accounts of "more than forty" customers of an unnamed "Technology Provider #1." The remaining counts allege that Weiss violated the same statute by accessing without permission and obtaining information from "more than 25" University of Michigan alumni email accounts (Count 23) and "more than five" accounts used by current or former students of Westmont College (Count 24).

Each of the counts in the indictment allege that the crimes occurred "in the Eastern District of Michigan and elsewhere."

Weiss's latest motion to dismiss raises issues of duplicity, multiplicity, and proper venue.

II.

Weiss brings his motion under Federal Rule of Criminal Procedure 12(b)(1), which allows a defendant to "raise by pretrial motion any defense, objection, or request" before trial that the court "can determine without a trial on the merits." Fed. R. Crim. P. 12(b)(1). Typically, those motions "involve[] questions of law instead of questions of fact on the merits of criminal liability." *United States v. Craft*, 105 F.3d 1123, 1126 (6th Cir. 1997). When addressing motions under Rule 12(b)(1), the Court "do[es] not evaluate the evidence upon which the indictment is based." *United States v. Landham*, 251 F.3d 1072, 1080 (6th Cir. 2001).

A.

Weiss first argues that Counts 21 through 24 should be dismissed as duplicitous because each of them alleges more than one distinct act of unauthorized computer access. He argues that this manner of charging deprives him of constitutionally required notice because each charge alleges multiple acts that would violate the target statute, and the prosecution has not specified which of the specific acts it intends to convict him on. That charging strategy, he says, would allow the government to elect the acts on which it seeks to convict him only after the evidence has been presented at trial. He also asserts that the government's manner of charging creates double jeopardy concerns because it is unclear which of the numerous alleged acts of cyber hacking actually are charged, and, therefore, the government could prosecute him for the same conduct in the future.

The government responds that each of the challenged counts charge but a single offense consisting of a course of conduct over a defined period and linked to a discrete victim (either individual victims, such as the Jane Does, or "institutional victims" in the case of the University of Michigan, Keffer Development Services, and other technology providers). It observes that this charging style is typical of prosecutions under 18 U.S.C. § 1030, where the possibility of increased punishment by charging each separate unauthorized intrusion is traded for efficiency. Any ambiguity, it insists, has been resolved by the extensive discovery materials provided; and any concern about jury unanimity can be addressed by jury instructions at trial. And the language of the indictment, the government contends, is so comprehensive that a conviction or acquittal on any of Counts 21 through 24 would bar future prosecutions for unauthorized computer access over the same date range and as to the same victims, thereby alleviating double jeopardy concerns.

All of the unauthorized computer access counts are brought under 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(ii), which are part of the Computer Fraud and Abuse Act (CFAA). That legislation prohibits "intentionally accesse[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). The statute applies to all "protected computers," including "all computers that connect to the Internet," *Van Buren v. United States*, 593 U.S. 374, 379 (2021), and website servers, *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1195 (9th Cir. 2022). Counts 21 through 24 of the indictment allege that Weiss violated sections 1030(a)(2)(C) and (c)(2)(B)(ii) by accessing without permission accounts hosted on various servers, obtaining information from them, and, in so doing, committing the tort of invasion of privacy under Michigan, Maryland, Pennsylvania, or California law.

"It is well-recognized that separate offenses must be charged in separate counts of an indictment." *United States v. Xu*, 114 F.4th 829, 838 (6th Cir. 2024) (quoting *United States v. Williams*, 998 F.3d 716, 734 (6th Cir. 2021)). "An indictment is deemed 'duplicitous' if it 'charges separate offenses within a single count. The overall vice of duplicity is that the jury cannot in a general verdict render its finding on each offense, making it difficult to determine whether a conviction rests on only one of the offenses or on both.'" *Ibid.* (quoting *United States v. Anderson*, 605 F.3d 404, 414 (6th Cir. 2010)).

A duplicitous indictment also may implicate the Sixth Amendment's guarantee of jury unanimity because it prevents the jury from convicting on one offense while acquitting on another. *Id.* at 838-39. "A defendant moving pursuant to Rule 12 can request that a duplicitous indictment be dismissed, he can attempt to force the government to elect the charge within the count upon which it will rely, or he can ask the court to particularize the distinct offenses contained within a count." *United States v. Kakos*, 483 F.3d 441, 444 (6th Cir. 2007) (citations omitted). Alternatively, the Court may mitigate the potential prejudice of a duplicitous indictment with a jury instruction explaining that unanimity is required as to the specific conduct giving rise to the offense. *Williams*, 998 F.3d at 735.

Weiss attacks Count 21 as duplicitous because it alleges that he compromised "approximately 150 accounts." Similarly, Counts 22 through 24 allege that he unlawfully accessed accounts belonging to "more than forty" of Technology Provider #1's customers, "more than 25" email accounts of University of Michigan alumni, and "more than five" accounts belonging to current or former students of Westmont College, respectively.

The government may allege that the defendant committed an offense "by one or more specified means." Fed. R. Crim. P. 7(c)(1). Therefore, "[i]t is not duplicitous to allege in one

count that multiple means have been used to commit a single offense." *United States v. Giampietro*, 475 F. Supp. 3d 779, 785 (M.D. Tenn. 2020) (quoting *United States v. Damrah*, 412 F.3d 618, 622 (6th Cir. 2005)). Prosecutors also may charge multiple violations of a statute in a single count as a "single, continuing scheme," unless doing so would expose the defendant to the "inherent dangers" duplicity poses, such as lack of unanimity, double jeopardy, lack of notice of the charges against him, or prejudicial evidentiary rulings. *United States v. Suarez*, 617 F. App'x 537, 544-45 (6th Cir. 2015) (quoting *United States v. Alsobrook*, 620 F.2d 139, 142 (6th Cir. 1980)). Courts generally leave to prosecutorial discretion the decision to charge a continuing scheme rather than discrete offenses. *Ibid.* However, if any of the "inherent dangers" are present, "the acts of the defendant should be separated into different counts even though they may represent a single, continuing scheme." *Id.* at 545 (quoting *Alsobrook*, 620 F.2d at 142). Even then, "[d]uplicitous indictments are not presumptively invalid; rather, duplicity is only reversible if it prejudices the defendant." *United States v. McNoriell*, 176 F.4th 413, 426 (6th Cir. 2026) (quotation marks omitted).

Weiss suggests that the government's charging strategy will prejudice him through a potential lack of unanimity among the jurors, the possibility of double jeopardy, and lack of notice. In this case, none of these concerns justify dismissing the challenged counts of the indictment.

As for unanimity, Weiss is correct that charging a "scheme" of multiple criminal acts in the same count raises the possibility that jurors could convict him without unanimous agreement on *which* of the criminal acts he committed. This is especially true when the number of charged discrete acts increases, since all jurors could agree that Weiss hacked into accounts, but they all might not agree on which ones. Here, the government apparently intends to present evidence of "more than 25" unauthorized logins alleged in Count 23. The same is true of the other "scheme"

counts — Counts 21, 22, and 24 — which allege many different unauthorized logins within a single count.

The possibility of lack of unanimity under these circumstances does not necessarily trench upon the Sixth Amendment. The Supreme Court has "never suggested that in returning general verdicts . . . the jurors should be required to agree upon a single means of commission, any more than the indictments were required to specify one alone." *Schad v. Arizona*, 501 U.S. 624, 631-32 (1991), *abrogated in part on other grounds as recognized in Edwards v. Vannoy*, 593 U.S. 255, 265 n.4 (2021). Even if the potential lack of unanimity is a cognizable form of prejudice in this case, the better way to address it is not dismissal, but rather a jury instruction explaining the jury's unanimity obligation. In *Alsobrook*, for example, the Sixth Circuit upheld a conviction where a single count of an indictment charged the defendant with six different trips that violated the Travel Act. The Court held that any unanimity problems were addressed sufficiently by an instruction reminding the jury that it must unanimously agree that at least one of the trips occurred in order to convict the defendant. *Alsobrook*, 620 F.2d at 143 ("[T]he district court, by instructing the jury that it must reach a unanimous decision on at least one act of interstate travel, obviated any possibility of a conviction based on a less than unanimous verdict."); *see also United States v. Blandford*, 33 F.3d 685, 699 (6th Cir. 1994) (upholding an extortion conviction where the defendant was charged with three payments, and the jury was told that a finding on one was sufficient to convict, but "all twelve of you must agree that the same one has been proved").

Nor is there a danger of exposing the defendant to double jeopardy. Counts 21 through 24 each allege a scheme of unauthorized computer access within a specified timeframe targeting customers of a designated technology provider. A conviction or acquittal would preclude further prosecution against Weiss for crimes committed within the boundaries of the scheme defined in

the indictment. *See*, *e.g.*, *United States v. Garcia-Limon*, 146 F.4th 885, 895 (10th Cir. 2025) (holding that two counts alleging numerous incidents of sexual abuse over the course of eight years did not present double jeopardy concerns because the government could not "subsequently charge [the defendant] with the same crimes against [the victim] during the eight-year period") (cleaned up); *United States v. Kamalu*, 298 F. App'x 251, 254 (4th Cir. 2008) (observing that a count in the indictment alleging a "continuing scheme" did not present double jeopardy concerns "because the Government is now foreclosed from prosecuting [the defendant] for further violations . . . that could form part of the alleged scheme"); *Hanf v. United States*, 235 F.2d 710, 715 (8th Cir. 1956) ("The rule against duplicitous pleading is not offended by a count charging more than one act if the acts were part of a transaction constituting a single offense. Certainly, any similar prosecution by the government against this appellant for a violation committed at any time between the dates indicated in Count 1 of the indictment would be a prosecution for the same offense, and would be promptly dismissed."). A future attempt by the government to prosecute Weiss for violations encompassed within the schemes alleged in Counts 21 through 24 likely would fail, since the government itself has admitted in its motion papers that a second prosecution for acts within the schemes would be barred by double jeopardy. *See* ECF No. 46, PageID.459.

Weiss also contends that the indictment does not adequately notify him of the charges against him because each of the challenged counts "aggregates numerous separate alleged entries into the same server without describing any of those entries, without identifying dates or times, and without distinguishing one access from another." ECF No. 30, PageID.151. Certainly, that charging style will make trial preparation more difficult if Weiss does not know ahead of time which of the numerous unauthorized login attempts alleged in the indictment the government actually intends to prove. However, when similar complaints have been made to support a request

for bills of particulars, courts have observed that "a defendant is not entitled to discover all the overt acts that might be proven at trial." *United States v. Salisbury*, 983 F.2d 1369, 1375 (6th Cir. 1993). And here, the government asserts that it has provided Weiss with extensive discovery "including documentation of specific intrusions," ECF No. 46, PageID.454, and Weiss does not dispute this in reply. It is fair to say, then, that Weiss has the information necessary to understand the charges against him and prepare for trial. *See United States v. Kandic*, 134 F.4th 92, 102 (2d Cir. 2025) (holding that duplicitous indictment charging the defendant with multiple deaths did not prejudice him where the deaths the government sought to prove at trial "were disclosed months, if not years, before trial").

Weiss also contends that charging the alleged CFAA violations as a "scheme" is improper under *Toussie v. United States*, which states that a crime should not be treated as a "continuing offense[]" unless "the explicit language of the substantive criminal statute compels such a conclusion, or the nature of the crime involved is such that Congress must assuredly have intended that it be treated as a continuing one." 397 U.S. 112, 115 (1970). *Toussie* used the term "continuing offense" to refer to a crime that continues to be committed following a completed act. The issue in that case was whether the defendant could be prosecuted in 1967 for failing to register for the draft in 1959, notwithstanding a five-year statute of limitations. *Id.* at 114. Whether the crime was deemed "continuing" turned on whether the statute supported the government's reading that the crime "continued to be committed each day that Toussie did not register." *Ibid. Toussie* does not illuminate the issue here, since there is no statute of limitations argument, and the case did not address whether multiple organized and serial criminal acts could be charged as a single scheme. The weight of authority suggests that the grand jury may charge in that manner. Fed. R. Crim. P. 7(c)(1); *Damrah*, 412 F.3d at 622-23; *Alsobrook*, 620 F.2d at 142.

Any prejudice that the defendant may perceive from charging the multiple violations of 18 U.S.C. § 1030(a)(2)(C) as a single "scheme" can be addressed at trial. It does not warrant dismissing Counts 21 through 24 of the indictment.

B.

Weiss next contends that Counts 21 through 23 should be dismissed as multiplicitous because they allege criminal conduct that already was alleged in other counts. He argues that all three counts expose him to double jeopardy because they can be proven through the same facts as counts alleged earlier in the indictment. Count 22, he observes, alleges hacking of "more than forty" customers of Technology Provider #1, when Counts 2, 7, 8, 9, and 10 also require the government to prove that he hacked customers of Technology Provider #1. Similarly, he observes that Count 23 alleges hacking of multiple University of Michigan accounts, which might overlap with the hacking alleged in Count 4. And Count 21 alleges that Weiss hacked into Keffer Development Services' servers, but allegations related to the Keffer hacking are "incorporated by reference" into Counts 1 through 10 in paragraph 15 of the indictment. He argues that all of these "defects" create the risk that he could be convicted twice for the same conduct, and this risk could not be cured by jury instructions, although he does not say why jury instructions would be insufficient.

The government contends that Weiss has not shown any factual overlap between Count 21 and the rest of the indictment. That count alleges hacks against Keffer Development Services, a victim not named in any other count, and Weiss only contends that it is multiplicitous because it incorporates by reference allegations used in support of other charges — a practice that expressly is permitted under Criminal Rule 7(c)(1) ("A count may incorporate by reference an allegation made in another count"). As to Counts 22 and 23, the government acknowledges that there may

be some overlap between those counts and earlier counts. For instance, Counts 2 and 7 through 10 allege that Weiss hacked accounts of customers of Technology Provider #1, which would overlap with the "more than forty" customers of Technology Provider #1 that Count 22 alleges were hacked. However, the government observes, there would be no overlap for at least 35 of the customers alleged in Count 22, and the Court could remedy any overlap at trial by merging the counts or providing a curative jury instruction. It makes the same argument for Count 23, which could overlap with the single University of Michigan accountholder in Count 4.

"Multiplicity occurs when a defendant is charged for 'a single offense in more than one count in an indictment.'" *United States v. Carter*, No. 22-5300, 2023 WL 2446140, at *2 (6th Cir. Mar. 10, 2023) (quoting *United States v. Myers*, 854 F.3d 341, 355 (6th Cir. 2017)). When the indictment charges the defendant under two different statutes for the same act or acts, courts use the elemental approach outlined in *Blockburger v. United States*, 284 U.S. 299, 304 (1932), analyzing "whether each charge requires proof of a fact that the other charge does not; if each charge does, then the charges accuse different crimes and are therefore not multiplicitous." *United States v. Montgomery*, No. 20-5891, 2022 WL 2284387, at *12 (6th Cir. June 23, 2022) (quoting *Myers*, 854 F.3d at 355).

Count 21 is not multiplicitous. It alleges that Weiss hacked into "virtual server space rented by the company Keffer Development Services," accessed certain personally identifying information, and then used the information to access other victims' accounts. Indictment, ECF No. 1, ¶22. The only reason that Weiss suggests this count is multiplicitous is because it incorporates by reference certain general allegations that also are incorporated by reference into Counts 1 through 10. But providing a set of background facts, followed by a list of specific counts — as the government has done here — is a standard pleading technique. It does not, by itself,

render the indictment duplicitous. None of the other counts seek to hold Weiss liable for unlawfully accessing Keffer Development Service's servers, so there is no risk that Weiss could be convicted twice for the crime alleged in Count 21.

On the other hand, Counts 22 and 23 might be multiplicitous because they both charge violations of 28 U.S.C. § 1030(a)(2)(c) and (c)(2)(B)(ii) that are also charged in other counts. Count 23 alleges that Weiss accessed "more than 25" University of Michigan email accounts between December 21, 2022 and December 23, 2022, while Count 4 also alleges an unauthorized login to a University of Michigan email account during December 2022. The indictment does not specify that the unauthorized logins alleged in Count 23 are different from the unauthorized login alleged in Count 4. Therefore, it at least is possible that Weiss could be convicted on Count 23 for the same act of unauthorized access alleged in Count 4, and neither charge strictly "requires proof of a fact that the other charge does not." *Montgomery*, 2022 WL 2284387, at *12 (quoting *Myers*, 854 F.3d at 355). A similar overlap occurs with Count 22 and Counts 2, 7, 8, 9, and 10. Therefore, based on the face of the indictment, Counts 22 and 23 may suffer from multiplicity.

But it does not automatically follow that dismissal of the offending counts is required. "The rule against multiplicity is a pleading rule, 'the violation of which is not fatal to an indictment.'" *United States v. Fisk*, 255 F. Supp. 2d 694, 702 (E.D. Mich. 2003) (quoting *United States v. Robinson*, 651 F.2d 1188, 1194 (6th Cir.1981)). If the government violates the rule, the defendant may "move to require the prosecution to elect either the count or the charge within the count upon which it will rely," or the Court may give an instruction "particularizing the distinct offense charged in each count in the indictment." *Robinson*, 651 F.2d at 1194. The Court also may defer the issue until after trial and enter judgment on only one of the convictions if it turns out that the defendant was convicted on two different counts based on identical conduct. *See Ball*

v. United States, 470 U.S. 856, 865 (1985); *Fisk*, 255 F. Supp. 2d at 703 ("The defendant's motion alleging multiplicity is premature. The government is entitled to proceed to trial on the indictment, but if convictions are returned on both counts 1 and 2, the government will be required to elect between the counts prior to sentencing."). Dismissal is not required at this juncture.

C.

Finally, Weiss contends that about half of the counts, namely Counts 1, 2, 6, 8, 9, 11, 12, 16, 18, 19, 21, and 22, must be dismissed because they do not specify that the alleged hacking occurred in the Eastern District of Michigan or that the targeted servers were located here. He asserts, without any authority, that "[a]llegations that an offense occurred 'in the Eastern District of Michigan and elsewhere' are insufficient where no essential conduct element is alleged to have occurred in this District." ECF No. 30, PageID.157.

The Court disagrees. It is true that "[t]he Constitution provides that the venue for a criminal prosecution must be the district where the crime was committed, and the government is required to establish venue by a preponderance of the evidence." *United States v. Iossifov*, 45 F.4th 899, 911 (6th Cir. 2022); U.S. Const. amend. VI; *see also* Fed. R. Crim. P. 18. "The necessity for proof of venue does not, however, require an allegation of venue in the indictment itself." *United States v. Branan*, 457 F.2d 1062, 1065 (6th Cir. 1972). "It is desirable for the indictment to allege the place where the crime was committed, but it is sufficient to state that the crime took place within the jurisdiction of the court and unnecessary to specify the city, county, or division." Wright & Miller's Federal Practice & Procedure § 126.

The government's allegations that all the crimes occurred "in the Eastern District of Michigan and elsewhere" sufficiently allege venue at this stage of the case. *See, e.g.*, *United States v. Minion*, No. 22-20059, 2023 WL 5437989, at *4 (E.D. Mich. Aug. 23, 2023) (allegation that

crimes occurred "in the Eastern District of Michigan and elsewhere" sufficiently alleged venue); *United States v. Coffman*, 652 F. Supp. 3d 911, 919 (S.D. Ohio 2023) (allegations that offenses occurred "within the Southern District of Ohio and elsewhere" sufficiently alleged venue at the pleading stage); *see also United States v. Grenoble*, 413 F.3d 569, 573 (6th Cir. 2005) (observing that "[a]ny defect in venue was . . . not apparent from the indictment itself" where indictment alleged that conduct took place "in the Northern District of Ohio"). The government says it will prove at trial that all of the unauthorized access attempts happened while Weiss lived and worked in the Eastern District of Michigan. If it does not offer such proofs, the defendant may seek relief at that time.

III.

None of the alleged pleading defects cited by the defendant warrant dismissal of any of the counts of the indictment.

Accordingly, it is **ORDERED** that the defendant's omnibus motion to dismiss certain counts of the indictment (ECF No. 30) is **DENIED**.

s/David M. Lawson
DAVID M. LAWSON
United States District Judge

Date: July 6, 2026